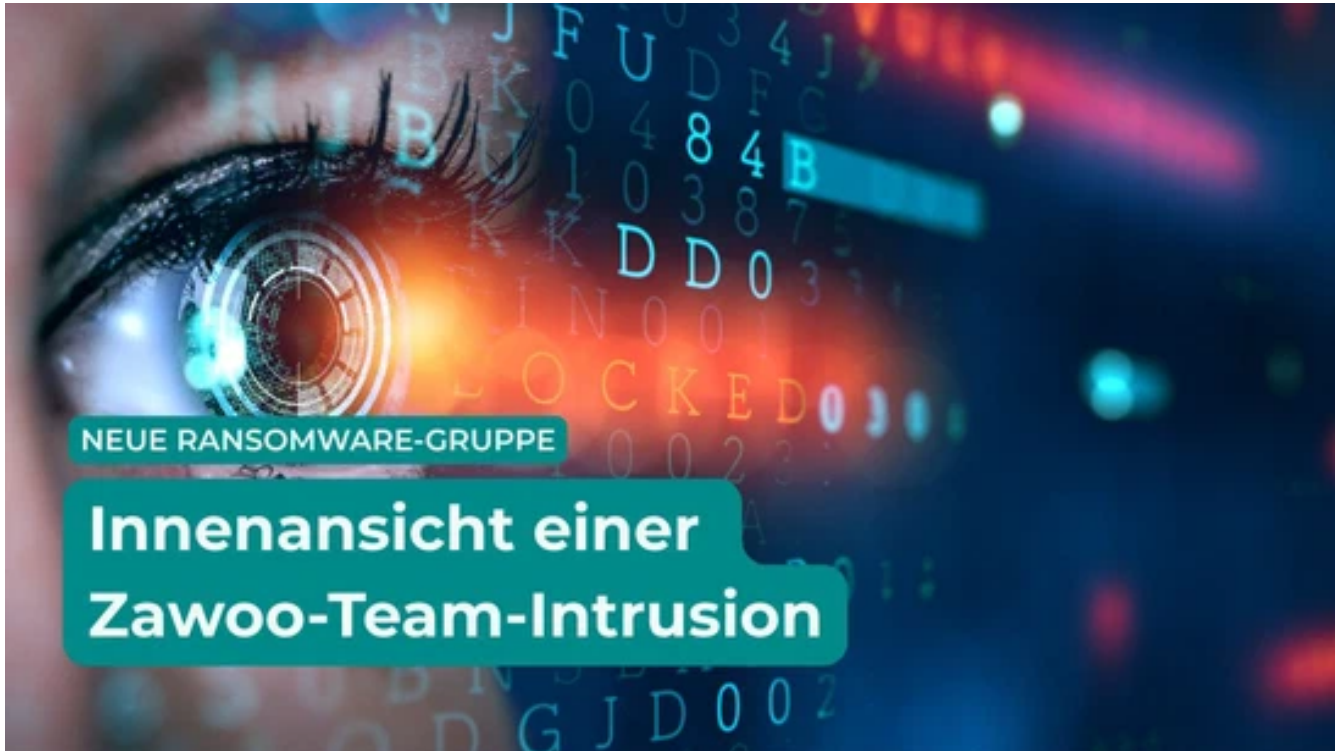


# Innenansicht eines Zawoo-Team-Angriffs

 [certainty.com/blog/zawoo-team-ransomware](https://certainty.com/blog/zawoo-team-ransomware)



- Veröffentlicht von Thomas Langthaler, Emirhan Sasmaz, Defensive Security
- 01 Sep
- Kategorie: [Blog](#)

*CERTAINITY, September 2026*

Redaktionshinweis: Hostnamen, Domains und interne Adressen wurden durch <domain>, <HOST>, 10.x.x.x ersetzt, die Dateiendung des Verschlüsselungsprogramms durch <EXT>. Details, die Rückschlüsse auf das betroffene Unternehmen oder dessen Branche zulassen würden, wurden entfernt.

## TL;DR

- **Wer:** Zawoo Team, spätestens seit Anfang August 2026 aktiv. Erst am 30. August ging die Leak-Site online, mit 19 Opfern auf einen Schlag, Schwerpunkt DACH-Region; laut ransomlook.io zählt die Gruppe zu den drei am stärksten trendenden. Vor diesem Zeitpunkt war über ihre Vorgehensweise beziehungsweise TTPs so gut wie nichts bekannt.

- **Dieser Fall:** wurde bearbeitet, bevor die Leak-Site online ging, wir “trafen” die Gruppe also zu einem Zeitpunkt, zu dem es keine öffentliche Berichterstattung gab. Durchgehend Hands-on-Keyboards, mit selbstgeschriebenen PowerShell-Tools (G-\*.ps1, Cp-\*.ps1), die in keinem öffentlichen Bericht auftauchen.
- **Erstzugriff:** gültige VPN-Zugangsdaten für ein bereits privilegiertes Konto, keine Multi-Faktor-Authentifizierung (MFA), weder Exploitation noch eine Escalation-Chain beobachtet. Wie die Zugangsdaten selbst erlangt wurden, bleibt unbekannt; eine Kompromittierung über Stealer-Logs ist generell ein plausibler Weg (laut Daten von ransomware.live/Hudson Rock sind auch 11,1 % der Zawoo-Opfer von Infostealern betroffen), für diesen konkreten Fall aber nicht bestätigt.
- **Fazit:** schnell und direkt statt raffiniert. Tippfehler in der Konsolen-History, ein mitten in der Session heruntergeladenes Tool, das ein bereits installiertes duplizierte, und am Ende wurde sogar der Staging-Host selbst verschlüsselt.
- Das vollständige ATT&CK-Mapping und alle Indikatoren finden sich am Ende dieses Beitrags.

Zawoo Team verschlüsselte mehrere Systeme und exfiltrierte Daten, hatte zu diesem Zeitpunkt aber noch keine Leak-Site, um sie zu veröffentlichen. Wir bearbeiteten den Angriff, als die Gruppe praktisch unsichtbar war: keine Leak-Site, keine öffentliche Berichterstattung, kein Name, der irgendjemandem etwas gesagt hätte. Inzwischen sind sie aus der Versenkung aufgetaucht. Was wir haben, ist die Evidenz eines einzelnen Falls dafür, wie sie tatsächlich vorgehen: das mitgebrachte Werkzeug, eine Reihe selbstgeschriebener PowerShell-Skripte, die in keinem öffentlichen Bericht auftauchen, und das, was die Konsolen-History ihrer Session hergibt.

Zawoo Team war spätestens seit Anfang August 2026 aktiv, möglicherweise auch schon früher, und agierte bis zum 30. August ohne Leak-Site. An diesem Tag stellten sie ihre ersten Opfer auf einen Schlag online. Die Site listet zum 30. August 19 Opfer mit Schwerpunkt auf der DACH-Region, und ransomlook.io führt die Gruppe unter den drei am stärksten trendenden Gruppen. Über ihre Tradecraft ist nach wie vor sehr wenig veröffentlicht.

Dies ist ein Einzelfall, kein Gruppenprofil. Wo wir etwas Allgemeineres über Zawoo aussagen, stammt es von deren Leak-Site oder aus öffentlichem Tracking, und wir kennzeichnen das entsprechend.

## Erstzugriff

---

Der Zugriff erfolgte über das VPN der Organisation, mit gültigen Zugangsdaten für ein bereits privilegiertes Konto. MFA war auf diesem VPN nicht erzwungen. Wir sahen weder Exploitation

noch eine Escalation-Chain: Das Konto meldete sich schlicht mit den Rechten an, die es bereits besaß.

Firewall-Logs waren nicht verfügbar, wie es leider so oft der Fall ist (hebt die verfluchten Logs auf!). Deshalb konnten wir nicht feststellen, wie die Zugangsdaten selbst erlangt wurden.

Die öffentlichen Daten liefern immerhin einen Hinweis darauf, woher Zugangsdaten für Opfer dieser Gruppe stammen könnten: ransomware.live erfasst für 11,1 % der Zawoo-Opfer eine Infostealer-Exposition. Diese Infostealer-Daten stammen im Rahmen einer Partnerschaft von Hudson Rock, es handelt sich also um eine Quelle, nicht zwei. Das macht Stealer generell zu einem plausiblen Weg, sagt aber nichts über unseren Fall aus. Dort bleibt der Weg unbekannt.

## Aufklärung

---

Die Angreifer öffneten die Netlogon-Skripte in SYSVOL, jene .cmd-Dateien, die Freigaben auf Laufwerksbuchstaben mounten. Sie lasen mehrere davon aus, kopierten dann eines unter neuem Namen und bearbeiteten es.

Netlogon-Skripte kann jeder authentifizierte Domänenbenutzer lesen, und in den meisten Umgebungen listen sie sämtliche Freigaben an einer Stelle auf. Wer herausfinden will, was sich mitzunehmen lohnt, hat damit eine nützliche Liste zur Hand.

Außerdem setzten sie Everything (voidtools) zur Datei- und Freigaben-Discovery ein, und leiteten die Ausgabe von `tree /a /f` in eine Datei um. Wir vermuten stark, dass sie genau diese Ausgabe nach der Veröffentlichung auf ihrer Leak-Site platzieren.

## Tooling

---

Der Angriff war durchgehend Hands-on-Keyboard. Wir konnten die Befehle aus der PSReadLine-Konsolen-History rekonstruieren

(%APPDATA%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost\_history.txt). Sie blieb erhalten, weil die Datei pro Benutzer geschrieben und bei jeder Befehlseingabe aktualisiert wird. Der Angreifer erbt damit die History des kompromittierten Kontos, seine Befehle stehen direkt hinter denen des Administrators.

Neben PsExec und RDP setzten sie DSInternals gegen einen Domain Controller ein und zogen zusätzlich einen SAM-nahen Registry-Export. DSInternals ist von beidem das folgenreichere Werkzeug: Gegen einen Domain Controller eingesetzt, kann es domänenweites Credential-Material extrahieren, dieselbe Zugriffsklasse wie ein DCSync-

artiger NTDS-Dump, statt nur der lokalen Konten eines einzelnen Hosts, die ein SAM-Export liefert. Ein erfolgreicher Lauf dort reicht aus, um die gesamte Domäne zu kompromittieren.

Zusätzlich verwendeten sie eine kleine Sammlung selbstgeschriebener PowerShell-Skripte:

| Skript              | Zweck                                      | Ausgabe                               |
|---------------------|--------------------------------------------|---------------------------------------|
| Cp-fs.ps1           | Sammlung von Dateifreigaben                | Ordner fs                             |
| Cp-pc.ps1           | Sammlung vom lokalen System                |                                       |
| G-WEBH.ps1          | Sammlung des Browserverlaufs               | BrowsingAudit_<YYYYMMDD>_<HHMMSS>.txt |
| G-hash-pth.ps1 <IP> | Pass-the-Hash, Ziel als Argument übergeben |                                       |

G- für get, Cp- für copy. Diese Namenskonvention haben wir in keinem öffentlichen Bericht gefunden.

Die Skripte löschten sich nicht selbst. Jedes wurde ausgeführt und anschließend von Hand entfernt:

```
.\Cp-fs.ps1  
del .\Cp-fs.ps1
```

Zur Defense Evasion setzten sie HRSword ein, ein legitimes kommerzielles Endpoint-Produkt des chinesischen Herstellers Huorong. Es wird als selbstextrahierendes Archiv ausgeliefert und registriert zwei Kernel-Treiber. HRSword ist ein weitverbreiteter Commodity-EDR-Killer und wurde bereits in Globelmposter- und Phobos-Angriffen dokumentiert. Die Herkunft des Tools sagt nichts darüber aus, wer es hier eingesetzt hat.

## Staging

Daten wurden in einen lokalen Staging-Ordner kopiert und in gesplittete 7z-Archive gepackt. Den Pack-Vorgang selbst haben wir nicht nachvollziehen können. Was darauf hindeutet: ein zu diesem Zeitpunkt auffällig hohes Schreibvolumen auf diesem Host in den Logs, der Staging-Ordner selbst und das anschließende Aufräumen.

Mitten in der Session luden sie Bandizip herunter, anstatt bereits vorhandenes Werkzeug zu verwenden. Das Archivformat verrät nicht, welches Tool es erzeugt hat, da sowohl Bandizip als auch 7-Zip 7z-Archive erzeugen.

## Exfiltration

---

Netzwerkbasierter Hinweise, dass Daten das Netzwerk verlassen haben, liegen uns nicht vor. Wie bereits erwähnt, wurden Firewall-Logs nicht lange genug aufbewahrt.

Was wir haben, ist ein gelöscht Archivfragment, das wir auf einem Host wiederherstellen konnten, sowie ein passender Dateiname auf der Leak-Site der Gruppe. Das macht Exfiltration auf diesem Wege sehr wahrscheinlich, beweisen können wir sie aus unserer eigenen Telemetrie aber nicht.

## Timeline

---

Soweit wir es sehen konnten, fand die Sammlung früh im Angriff statt, die Verschlüsselung folgte mehrere Tage später. Unsere Sichtbarkeit war eingeschränkt, die tatsächliche Verweildauer (Dwell Time) kann also durchaus länger sein als die uns vorliegenden Daten nahelegen. Die früheste von uns gefundene Aktivität ist nicht zwangsläufig die früheste, die es gab.

Der Host, von dem aus die Angreifer agierten, wurde am Ende ebenfalls verschlüsselt.

## Verschlüsselung und Erpressung

---

Die Ransomware selbst konnten wir nicht sicherstellen, ebenso wenig den Weg nachvollziehen, wie sie auf die Hosts verteilt wurde, auf denen sie lief. Ein Sample liegt auf VirusTotal ([dd21e22e...e337e](#)). Verschlüsselte Dateien wurden in eine 16-stellige Hex-Zeichenfolge mit angehängter neuer Dateiendung umbenannt, z. B. a1b2c3d4e5f6a7b8.<EXT>.

Die Ransom Note trug den Namen `How to restore your files.txt` und verwies für die Kontaktaufnahme auf den Messenger Session mit einer Angriffs-spezifischen ID, mit `zawooorestore@onionmail.org` als Fallback.

Die von uns sichergestellte Note ist nicht dieselbe wie in der öffentlichen Berichterstattung. PCrsk dokumentierte am 12. August 2026 ein Zawooo-Sample mit der Adresse `zawooorecover@onionmail.org` und deutlich abweichendem Wording: Diese Variante stellt die Gruppe als „eine Ransomware, die Wert auf ihren Ruf legt“ dar und droht, gestohlene Dateien und Postfachinhalte an die Kunden des Opfers zu versenden. Unsere Note enthält

keines von beidem. Das Schema der Dateiumbenennung stimmt in beiden Fällen überein, das ist der belastbarere Indikator. Behandeln Sie Wortlaut der Note und Kontaktadresse als variantenspezifisch, und nutzen Sie keines von beidem, um einen Zawoo-Fall ein- oder auszuschließen.

Unsere Note, mit entfernter Opfer-ID und einer branchenidentifizierenden Zeile (im englischen Original, unverändert übernommen):

```
-- Hello, From Zawoo Team
your ID : [REDACTED]
Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data
We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreement, your data
will be published.
Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank
statements.
- [REDACTED: line naming file formats specific to the victim's sector]
- And more...

-- Warning
1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key.
   We encourage you to consider your decisions.

-- How to contact us ?
1) Download Session: https://getsession.org/download and Click New Messages,
   Contact with ID : [REDACTED]
2) Send email      : zawooorestore@onionmail.org
```

Rechtschreib- und Grammatikfehler sind wie im Original wiedergegeben.

## Was wir daraus mitnehmen

---

Die Arbeit war Hands-on-Keyboard und nicht besonders sorgfältig. Die Konsolen-History enthält Tippfehler, einen Befehl für nicht installierte Software und eine dreifach eingefügte Zeile. Die Angreifer verschlüsselten den Host, von dem aus sie gearbeitet hatten. Zum Zeitpunkt des Vorfalls hatte die Gruppe noch keine Leak-Site, drohte also mit einer Veröffentlichung, für die es noch gar kein Ziel gab.

Die Leak-Site als Ganzes wirkt organisierter als die Angreifer-Session, die wir nachvollziehen konnten. Unser eigener Fall fällt ein wenig aus dem Muster, was uns daran erinnert, dass ein einzelner Fall nicht immer zwingende Rückschlüsse auf die Gewohnheiten einer Gruppe zulässt. Wir würden daraus keine Rückschlüsse auf ihre Gesamtfähigkeiten ziehen. Neu im Geschäft sind sie aber allemal, es ist gut möglich, dass sie sich von hier aus noch „verbessern“.

## Detection

---

Wonach sich basierend auf unseren Beobachtungen suchen lässt:

- G-\*.ps1- und Cp-\*.ps1-Skriptnamen, ausgeführt und anschließend manuell gelöscht
- BrowsingAudit\_<timestamp>.txt
- Everything.exe oder bandizip.exe auf einem Server
- HRSword-Artefakte: sysdiag.sys, hrwfpdrv.sys, usysdiag.exe
- PSEXESVC-Dienstinstallation, Event-ID 7045
- DSInternals-Modul-Load auf einem Domain Controller
- Änderungen an Netlogon-Skripten in SYSVOL (auditierbar, aber selten überwacht)
- PSReadLine-Konsolen-History, bevor sie überschrieben wird

## Anhang

---

### Indikatoren

---

Variantenspezifische Indikatoren sind gekennzeichnet. Verlassen Sie sich nicht allein auf diese.

| Typ         | Indikator                     | Hinweis                                         |
|-------------|-------------------------------|-------------------------------------------------|
| E-Mail      | zawooorestore@onionmail.org   | unser Fall                                      |
| E-Mail      | zawooorecover@onionmail.org   | PCrisk-Sample, 12. Aug. 2026                    |
| Messenger   | Session, opferspezifische ID  | variantenspezifisch                             |
| Ransom Note | How to restore your files.txt | Groß-/Kleinschreibung variiert je nach Variante |

| Typ              | Indikator                                                                   | Hinweis                                               |
|------------------|-----------------------------------------------------------------------------|-------------------------------------------------------|
| Dateiumbenennung | 16-stelliger Hex-Name, angehängte neue Dateiendung (a1b2c3d4e5f6a7b8.<EXT>) | über alle Varianten konsistent                        |
| Leak-Site        | Top-Level-Ordner FsTmp und right                                            | bei rund der Hälfte der Zawoo-Opfer; nicht unser Fall |
| Dateiname        | BrowsingAudit_<YYYYMMDD>_<HHMMSS>.txt                                       | Ausgabe von G-WEBH.ps1                                |
| Skript           | Cp-fs.ps1, Cp-pc.ps1, G-WEBH.ps1, G-hash-pth.ps1                            | eigenentwickelt, nach Gebrauch von Hand gelöscht      |
| Treiber          | sysdiag.sys, hrwfpdrv.sys                                                   | HRSword                                               |
| Binary           | usysdiag.exe                                                                | HRSword                                               |

# SHA-256

11B262C936FFA8EB83457EFD3261578376D49D6E789C7C026F1FA0B91929E135 sysdiag.sys (HRSword)

dd21e22e2c4fffc5939dc6e42ee42ed497138d17245b59dcf4b0aca9739e337e Zawoo-Verschlüsseler (VirusTotal, von uns nicht sichergestellt)

# E-Mail

zawooorestore@onionmail.org

zawooorecover@onionmail.org

## ATT&CK-Mapping

Basierend auf dem, was wir in diesem Fall direkt beobachtet haben. Initial Access und Exfiltration sind enthalten, weil sie für die Gesamtabdeckung relevant sind, auch wenn wir den jeweiligen Mechanismus nicht bestätigen konnten.

| Taktik         | Technik        | ID    | Evidenz                                                                                                                              |
|----------------|----------------|-------|--------------------------------------------------------------------------------------------------------------------------------------|
| Initial Access | Valid Accounts | T1078 | VPN-Login mit gültigen, bereits privilegierten Zugangsdaten; kein MFA erzwungen; keine Exploitation oder Escalation-Chain beobachtet |

| <b>Taktik</b>     | <b>Technik</b>                                       | <b>ID</b> | <b>Evidenz</b>                                                      |
|-------------------|------------------------------------------------------|-----------|---------------------------------------------------------------------|
| Discovery         | Network Share Discovery                              | T1135     | Netlogon-/SYSVOL-Skripte gelesen; Everything (voidtools) ausgeführt |
| Discovery         | File and Directory Discovery                         | T1083     | Ausgabe von tree /a /f in eine Datei umgeleitet                     |
| Credential Access | OS Credential Dumping: Security Account Manager      | T1003.002 | SAM-naher Registry-Export                                           |
| Credential Access | OS Credential Dumping: NTDS                          | T1003.003 | DSInternals gegen einen Domain Controller ausgeführt                |
| Lateral Movement  | Remote Services: SMB/Windows Admin Shares            | T1021.002 | Psexec, PSEXESVC-Dienstinstallationen (Event-ID 7045)               |
| Lateral Movement  | Remote Services: Remote Desktop Protocol             | T1021.001 | RDP in der Konsolen-History beobachtet                              |
| Lateral Movement  | Use Alternate Authentication Material: Pass the Hash | T1550.002 | G-hash-pth.ps1 <IP>                                                 |
| Collection        | Data from Network Shared Drive                       | T1039     | Cp-fs.ps1                                                           |
| Collection        | Data from Local System                               | T1005     | Cp-pc.ps1                                                           |
| Collection        | Browser Information Discovery                        | T1217     | G-WEBH.ps1, Ausgabe BrowsingAudit_<timestamp>.txt                   |

| Taktik          | Technik                                  | ID        | Evidenz                                                                                                      |
|-----------------|------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------|
| Collection      | Archive Collected Data                   | T1560     | Gesplittete 7z-Archive via 7-Zip und Bandizip                                                                |
| Defense Evasion | Impair Defenses: Disable or Modify Tools | T1562.001 | HRSword, Kernel-Treiber<br>sysdiag.sys/hrwfpdrv.sys                                                          |
| Defense Evasion | Indicator Removal                        | T1070     | Skripte nach jedem Lauf manuell gelöscht                                                                     |
| Exfiltration    | Exfiltration Over Web Service            | T1567     | Nicht bestätigt, abgeleitet aus gelöschtem Archivfragment und übereinstimmendem Dateinamen auf der Leak-Site |
| Impact          | Data Encrypted for Impact                | T1486     | Dateien mit 16-stelligem Hex-Namen und <EXT>-Dateiendung umbenannt                                           |

**Quellen:** CERTAINITY-Falldaten · [ransomware.live](#) · [ransomlook.io](#) · [PCrisk](#) · [Hudson Rock](#)

## Kategorien

- [Blog \(28\)](#)
- [Interview \(12\)](#)
- [News \(2\)](#)
- [Podcast \(1\)](#)

## Tags

- [active directory \(1\)](#)
- [adcs \(1\)](#)
- [ai \(2\)](#)
- [assessment \(2\)](#)
- [bcm \(1\)](#)
- [bec \(1\)](#)
- [cert \(1\)](#)
- [cra \(1\)](#)
- [cyber resilience act \(1\)](#)

- [cyberversicherung \(1\)](#)
- [data act \(1\)](#)
- [datenschutz \(2\)](#)
- [ddos \(3\)](#)
- [dfir \(1\)](#)
- [digitale souveränität \(1\)](#)
- [dsgvo \(1\)](#)
- [europa \(1\)](#)
- [identitätsdiebstahl \(1\)](#)
- [incident response \(4\)](#)
- [incident simulation \(1\)](#)
- [initial compromise \(2\)](#)
- [iocs \(1\)](#)
- [iso27001 \(3\)](#)
- [jahresausblick \(8\)](#)
- [ki \(1\)](#)
- [kmu \(2\)](#)
- [kooperation \(1\)](#)
- [nis2 \(1\)](#)
- [osint \(1\)](#)
- [pentesting \(2\)](#)
- [pharma \(1\)](#)
- [pre-employment-screening \(1\)](#)
- [ransomware \(2\)](#)
- [red teaming \(6\)](#)
- [responsible disclosure \(1\)](#)
- [secure development \(2\)](#)
- [security awareness \(2\)](#)
- [team zawoo \(1\)](#)
- [threat modeling \(3\)](#)
- [ttps \(1\)](#)
- [zeroobs \(1\)](#)